IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DATA SECURITY IN WSN USING SYMMETRIC KEY AP ALGORITHM

[1]Pawan Kumar Goel, [2]Prof. (Dr.) Sarvottam Dixit

1. Research Scholar, Department of CSE, Mewar university Rajasthan, India

2. Pro-Vice-Chancellor, Mewar University, Rajasthan, India

Abstract: Data security and confidentiality are crucial aspects of WSN's. As a result, the invader will not be able to disrupt the data. The data discovery and dissemination protocol for wireless sensor networks is in charge of changing configuration parameters and disseminating management directives. However, one disadvantage is that some protocols were not designed with security in mind. As a result, the D3D protocol is introduced, which is the first safe and distributed data discovery and dissemination protocol. This protocol's main purpose is to allow many network users to be authorized. As a result, the system provides a high level of security to the wireless sensor network by utilizing several security factors. Because it is tough to crack, a novel energy-efficient algorithm is also used.

Keywords: D3D Protocol, WSN

I. Introduction

Wireless sensor networks are a highly distributed network of all small and light-weighted nodes that measure physical characteristics such as temperature, pressure, and relative humidity and are dispersed across the system in huge numbers. Each sensor node in the network is made up of three subsystems: a sensor subsystem that senses the environment, a processing subsystem that performs local computations on the sensed data, and a communication subsystem that exchanges messages with surrounding sensor nodes [1]. WSNs can be used for a variety of tasks, including environmental monitoring, military zones, sensitive sites, and remote data collecting and processing. Data distribution is the most critical process in a sensor network. Queries and data are routed through the sensor network. Sensor nodes must communicate with any other node that is interested in the data, such as a base station, in order to collect data. The source's job is to generate data, and events can be run when information has to be reported. The way a sink works is that it is used by a node that is interested in an event and wants to learn more about it.

System initialization, user joining, packet pre-processing, and packet verification are the four phases of D3D protocol. The network owner creates its public and private keys in the system initialization phase for our basic protocol, and then loads the public parameters on each node before the network deployment. A user gains dissemination privilege by registering with the network owner during the user joining phase. If a user joins the network and wants to disseminate some data, he or she must first generate the data dissemination packets and

then send them to the nodes during the packet pre-processing phase. A node verifies each received packet during the packet verification phase. If the result is positive, the data is updated according to the packet received.

Following the deployment of a wireless sensor network (WSN), it is common to need to update buggy/old small applications or parameters stored in the sensor nodes. This is accomplished using the data discovery and dissemination protocol, which allows a source to send short programmes, commands, queries, and configuration settings to sensor nodes. The data discovery and dissemination protocol is in charge of changing configuration parameters and distributing management commands.

The remaining of the paper is organized as follows: The related work is described in Section II. The proposed design is shown in Section III. The implementation setup is described in Section IV. The graph is presented in Section V, and the last section, i.e. The conclusion is presented in Section VI.

II. Related Work

A first secure and distributed data discovery and dissemination protocol is presented by D. He, S. Chan, Mohsen Guizani, and H. Yang [2]. It will allow the network owner to permit several network users with various privileges to the sensor node to simultaneously and directly disseminate data items, and it will address a number of possible security vulnerabilities.

D. He, S. Chan, S. Tang, and M. Guizani [5], they had proposed the identification of the security vulnerabilities in data discovery and dissemination when used in WSNs. An attacker can use these flaws to inject unwanted values into a network, remove critical variables, or perform denial-of-service assaults. To solve these flaws, this study describes the design and assessment of SeDrip, a secure, lightweight, and DoS-resistant data discovery and dissemination protocol for wireless sensor networks. This protocol takes into account the sensor nodes' limited resources, packet loss, and out-of-order packet delivery. It can also give instantaneous authentication because there is no packet buffering latency and it tolerates node compromise.

John Paul Walters, Zhengqiang Liang, Weisong Shi, and V. Chaudhary, These types of researches have been done because wireless sensor networks require appropriate security mechanisms. Because sensor networks may interact with sensitive data and function in an unattended hostile environment, security problems must be addressed from the start of the system design. They argued that the Wireless Sensor Network security highlights the difficulties and requirements in sensor security.

III. Proposed Design

Algorithm Proposed

The suggested technique is a new symmetric key AP algorithm that uses shuffling, substitution, and shifting to create an energy-efficient and difficult-to-crack security mechanism for WSN. The encryption and decryption algorithms are as follows.

Algorithm for AP Encryption

1. Given Plain Text.
2. Randomly generate key k
3. Calculate key K2 and key 3 from the key k.
4. Repeat
5. Divide the n bits of plain text P into r blocks of key size k, so that n= k*r + m, where m is the modulus (n, k)
6. Shuffle r blocks using key K.
7. Substitute the text (n bits) using key K2
8. Shift the text in a circular left shift with k3
9. until all round done.

Algorithm for AP Decryption

1. Given Cipher Text and key k
2. Calculate key k_inv, k2 & k3 from the key k.
3. Repeat
4. Shift the text in circular right shift with k3
5. Substitute the text (n bits) using key k2.
6. Divide the n bits of plain text P into r multiple blocks of key size k such that n = k * r + m where m is mod (n, k)
7. Shuffle r blocks using inverse key k_ inv
8. until all round done.

The following is the proposed design, which is divided into three parts:

A) Formation and Communication of Wireless Sensor Networks ,
B) D3D (Data Discovery and Dissemination Protocol) and Parameter Requirements, and
C) WSN Security

A. Formation and Communication of Wireless Sensor Networks

This step involves constructing a comprehensive wireless sensor network, which includes determining the number of Sensor Nodes, Storage Nodes, and Sink Nodes, as well as interconnecting them to form the network.

Following the completion of the Wireless Sensor Network design, the following stage is to establish communication between all nodes, storage node, and sink node. The communication in the sense that data will be transmitted between distinct nodes inside the node.

B. Data Discovery and Dissemination Protocol (D3D Protocol) and Parameter Requirements

The proposed design will place a focus on the distribution of data discovery and dissemination protocols, as well as the realisation of their functional requirements and the definition of their design goals. Identify security flaws in existing data discovery and dissemination techniques as well.

C. Providing the Security to WSN

The suggested module is a symmetric key block cypher method. Shuffling, substitution, and shift left are the three 3S operations that must be executed to the plain text in each round. The number of rounds might range from 2^0 to 2^10. Plain Text can be as long as you want it to be. Despite the fact that it is a block cypher, the suggested technique does not require any padding.

Shuffling

To shuffle the plain text, the algorithm first produces a permutation table using a P-box of size 48 bits in this module. As a result, a key space of 48 bits, i.e.1.2414e + 061, is created, which is large enough for the intruder to crack. To demonstrate how the algorithm works, a 16-bit key is used as an example.

Substitution

Substitution is performed by using Vigenere Cipher. Vigenere Cipher is a poly alphabetic substitution where text is encrypted using a series of additive cipher. An additive cipher is a traditional cipher where text is shifted ahead to a particular number. Text 'M 'is substituted to 'U' for additive key = 8.

Shift

The circular shift is performed to the cypher text created in the previous phase, and the amount of shifts depends on the key K2 used by Vigenere cypher. The leftmost digit of key k2 is key k3 for circular left shift. k3 = most to the left (K2). In the example, k3 = 9 and the final encrypted text was formed.

Requirements for Security

• Data confidentiality

Sensor data from neighbouring networks should not be shared. Nodes can exchange highly sensitive data in a variety of applications. It achieves confidentiality by encrypting sensitive data with a secret key that is only intended for the receivers.

• Data authentication

Message authentication is critical for many applications in sensor networks. In any decision-making process, data comes from a reliable source that must be verified by the receiver. Because a foe can simply inject messages. A receiver can verify that the data was sent by the claimed sender using data authentication.

• Integrity of data

Data integrity in communication can be assured by the receiver that the received data has not been tampered with in transit by an adversary. During the data distribution process, a sensor should be able to confirm that received data items have not been updated.

IV. Experimental Setup

A. *Simulation Environment*

The simulation environment used to analyse the proposed system is called NS2. The Network Simulator-2 (NS2) is an event-driven simulation tool for studying the dynamic dynamics of communication networks. In NS2, you can simulate both wired and wireless network services and protocols. In NS2, two main languages are C++ and Object-oriented Tool Command Language (OTcl). After a simulation, NS2 generates text-based simulation results.

There are tools available to evaluate these results graphically and interactively, such as NAM (Network AniMator) and XGraph.

To analyse a certain network behaviour, the user can extract text-based data. The parameters used in the simulation process for this proposed system are listed in TABLE I:

Routing Protocol	**AODV**
Simulation Time	**80 seconds**
Simulation Area	**1500 X 1000 m^2**
Number of Nodes	**80**
Traffic Type	**CBR**
Pause Time	**0.2 Seconds**
Mobility	**10 meter/ sec**
Packet Size	**512 bits**
Data rate	**512 kbps**
Queue Model	**Priority Queue**
MAC	**802.11(a)**
Channel Type	**Wireless Channel**

Table I: Simulation parameter

B. Outcomes

The screen shots taken during network formation are shown below.

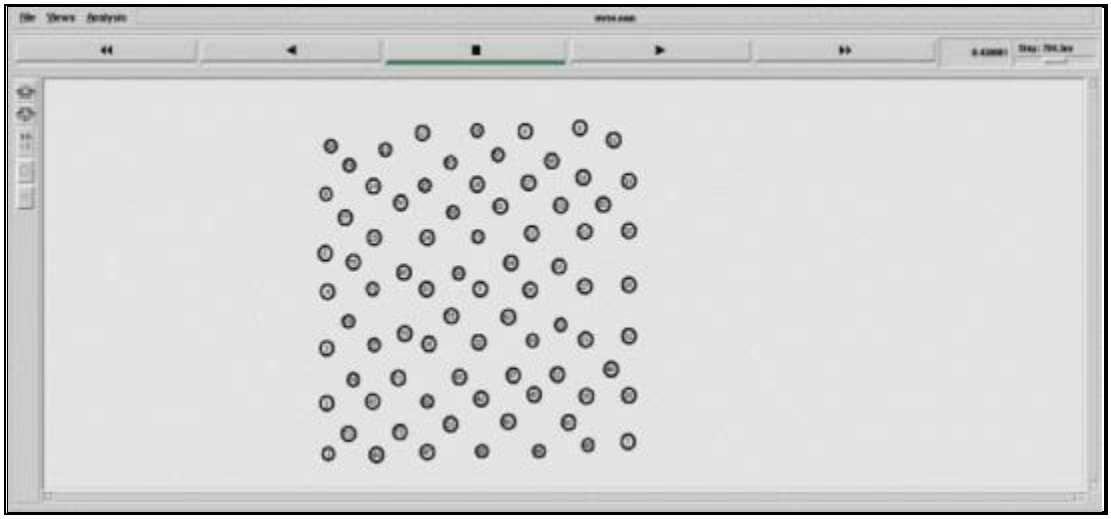

Fig. 1: Formation of network

Here in Figure1, With the help of the network animator, all of the nodes are created and a network is formed. A total of 80 nodes are used to build the network.

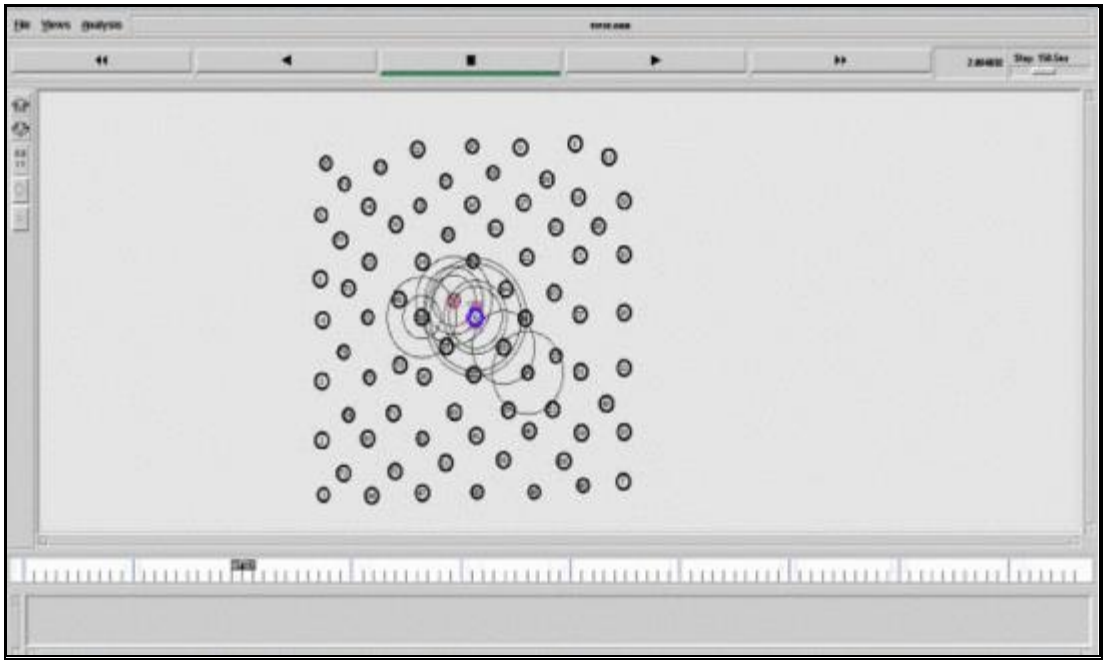

Fig. 2: Communication between nodes

In Figure2, Once the network has been built, nodes can communicate by sending requests.
If the request is accepted by the neighboring node, the color of that node will change.

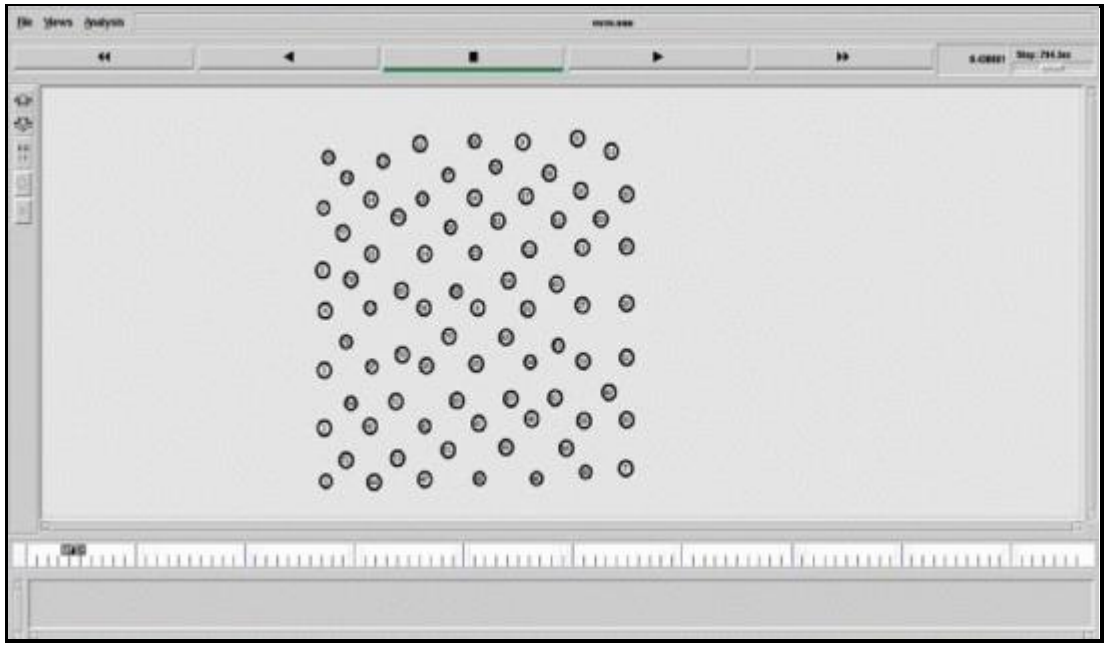

Fig. 3: Detection of malicious node

In figure3, It's tough to tell whether a node is malicious or not in a network. However, malicious nodes are recognized and deleted using the AP method.

V. Graph

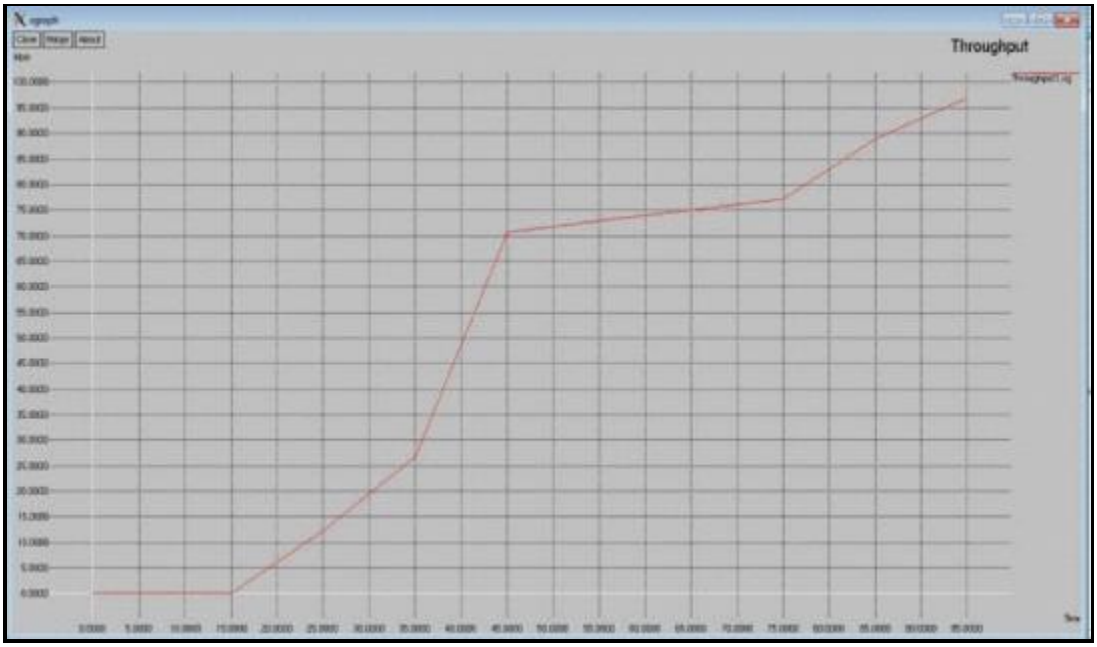

Fig. 4: Experimental graph showing the analysis of throughout.

In figure4, the analysis of throughout is calculated with the help of graph which indicates that throughout is goes on increasing.

Comparative Analysis:

Comparison Table between AP and AES algorithm.

S.No.	Parameters	Algorithms	
		AP	AES
1	No. of CPU Cycle	LESS	HIGH
2	Key Size	LOW	HIGH
3	Energy Consumption	LESS	HIGH
4	Throughout	HIGH	LESS

Table II: Comparison of AP and AES algorithm

VI. Conclusion:

Considering such a problem with wireless sensor networks in terms of security, which is more complex and difficult in nature, as well as security weaknesses in data discovery and dissemination when employed in WSNs. A novel AP algorithm that uses less energy has been proposed. Thus, in the design of secure and distributed data discovery and dissemination protocols, as well as the AP algorithm, we will address how to preserve data secrecy, and the system will retain data integrity while also ensuring system performance.

We can conclude from this that the suggested system will provide great security. The message can then be encrypted and decrypted for security purposes using an energy-efficient new technique. We suggested a new symmetric key AP technique based on shuffling, substitution, and shifting to represent a WSN security system that is both energy efficient and difficult to crack. We will not only detect the malicious node in the network, but we will also delete the attacker node, making the system far more safe and trustworthy. By detecting and removing the attacker from the wireless sensor network, we will have a high level of security. The study was carried out using a network simulator (NS2).

REFERENCES

[1] D. He, S. Chan, Mohsen, Guizani, H. Yang, “Secure and distributed data discovery and dissemination in Wireless Sensor Network”, IEEE Trans. Parallel and distributed system, 2014.
[2] D. He, C. Chen, S. Chan and J. Bu, “DiCode: DoS resistant and distributed code dissemination in wireless sensor networks”, IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946-1956, May 2012.
[3] D. He, S. Chan, S. Tang, and M. Guizani, “Secure data discovery and dissemination based on hash tree for wireless sensor networks,” IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638-4646, Sept. 2013.
[4] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, “Wireless Sensor Network Security: A Survey”,
Department of Computer Science Wayne State University, 2006 Auerbach Publications, CRC Press. [2] D. He, S. Chan, Mohsen, Guizani, H. Yang, “Secure and distributed data discovery and dissemination in Wireless Sensor Network”, IEEE Trans. Parallel and distributed system, 2014
[5] Archana Tayal, Prachi , “Energy Efficient New Symmetric Key Algorithm (AP) for WSN”, Research Notes in Information Science (RNIS) Volume13, May 2013 doi:10.4156/rnis.vol13.35.
[6] D. He, C. Chen, S. Chan and J. Bu, “DiCode: DoS resistant and distributed code dissemination in wireless sensor networks”, IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946-1956, May 2012.
[7] D. He, S. Chan, S. Tang, and M. Guizani, “Secure data discovery and dissemination based on hash tree for wireless sensor networks,” IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638-4646, Sept. 2013.

[8] Archana Tayal, Prachi , "Energy Efficient New Symmetric Key Algorithm (AP) for WSN", Research Notes in Information Science (RNIS) Volume13, May 2013 doi:10.4156/rnis.vol13.35.
[9] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey",
Department of Computer Science Wayne State University, 2006 Auerbach Publications, CRC Press.